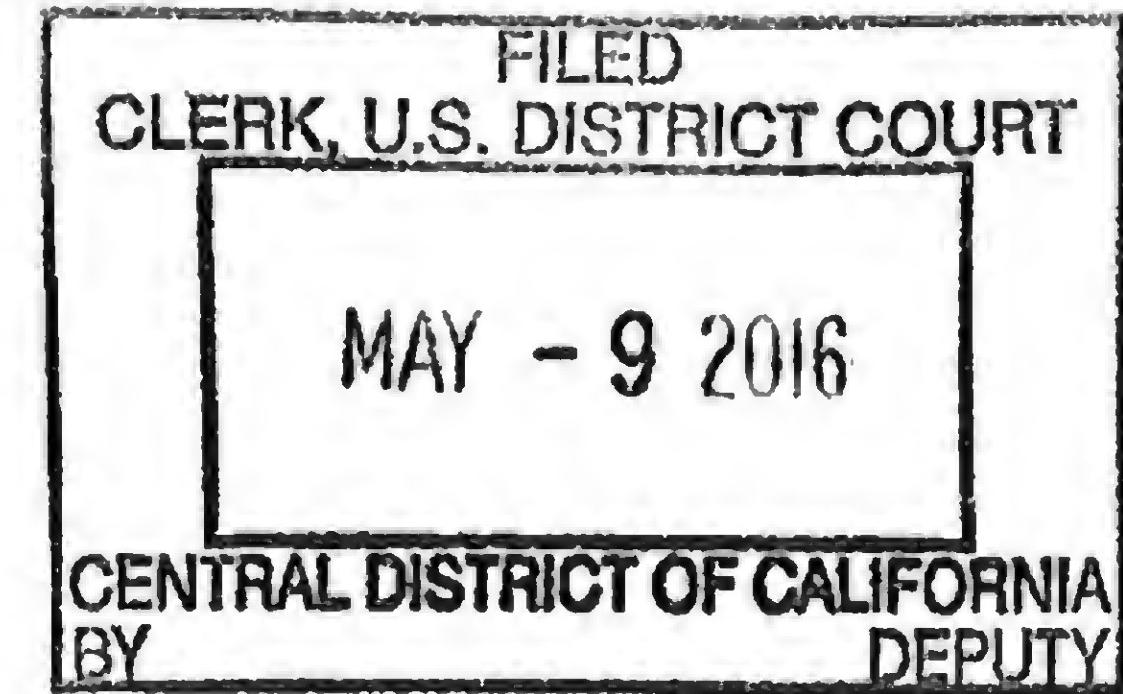


1 EILEEN M. DECKER  
2 United States Attorney  
3 LAWRENCE S. MIDDLETON  
4 Assistant United States Attorney  
5 Chief, Criminal Division  
6 J. MARK CHILDS (Cal. Bar No. 162684)  
7 Assistant United States Attorney  
8 OCDETF Section  
9 1400 United States Courthouse  
10 312 North Spring Street  
11 Los Angeles, California 90012  
12 Telephone: (213) 894-2433  
13 Facsimile: (213) 894-0142  
14 E-mail: mark.childs@usdoj.gov



15 Attorneys for Plaintiff  
16 UNITED STATES OF AMERICA

17 PH C  
18 G  
19 I  
20 IN RE THE SEARCH OF [REDACTED]  
21 NO. [REDACTED]

22 20 200 20  
23 20 200 20

24

25

26

27

28

UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA

29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889

1 application and search warrant filed in this matter, and such further  
2 evidence and argument as the Court may permit.

3 Dated: May 9, 2016

Respectfully submitted,

4 EILEEN M. DECKER  
United States Attorney

5 LAWRENCE S. MIDDLETON Assistant  
United States Attorney  
Chief, Criminal Division

6  
7 /s/  
8 J. MARK CHILDS  
9 Assistant United States Attorney

10 Attorneys for Plaintiff  
UNITED STATES OF AMERICA

## MEMORANDUM OF POINTS AND AUTHORITIES

## I. INTRODUCTION

3 The government submits this supplemental authority in support of  
4 its application for a search warrant which seeks authorization to  
5 depress the fingerprints and thumbprints of every person who is  
6 located at the SUBJECT PREMISES during the execution of the search  
7 and who is reasonably believed by law enforcement to be a user of a  
8 fingerprint sensor-enabled device that is located at the SUBJECT  
9 PREMISES and falls within the scope of the warrant. The government  
10 seeks this authority because those fingerprints, when authorized by  
11 the user of the device, can unlock the device.

12 This procedure will not vi Attached hereto is an article from  
13 the Daily Journal dated Friday, May 6, 2016, entitled "Thumbprints to  
14 unlock phones can be compelled, courts say."

## II. FACTUAL BACKGROUND

In the affidavit in support of the search warrant, the affiant states that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not

1 necessarily from the same person, will unlock the device. If there  
2 is no sensor on the device, the device will not open with prints.

3 There are limits on the ability to use a fingerprint or  
4 thumbprint to unlock a device, which varies by manufacturer. For  
5 example, with Apple, the Touch ID feature only permits up to five  
6 attempts with a print before the device will require the user to  
7 enter a passcode. Furthermore, the Touch ID feature will not  
8 substitute for the use of a passcode or password if more than 48  
9 hours have passed since the device has been unlocked; in other words,  
10 if more than 48 hours have passed since the device was accessed, the  
11 device will require the passcode or password programmed by the user  
12 and will not allow access to the device based on a print alone.  
13 Similarly, Touch ID will not allow access if the device has been  
14 restarted or was off and has been turned on, if the device has  
15 received a remote lock command, or if five attempts to match a print  
16 have been unsuccessful. Other brands have similar restrictions.

17 In order to attempt to gain access to the devices found at the  
18 SUBJECT PREMISES, the search warrant seeks the authority to use the  
19 fingerprints and thumbprints of any person who is located at the  
20 SUBJECT PREMISES during the execution of the search and who is  
21 reasonably believed by law enforcement to be a user of a fingerprint  
22 sensor-enabled device that is located at the SUBJECT PREMISES and  
23 falls within the scope of the warrant. Without the numerical or  
24 alpha-numerical passcode, the government may not be able to obtain  
25 the contents of the devices if those prints are not used.  
26 Furthermore, delaying action may prevent even the use of this method  
27 of gaining access if that delay prevents the government from  
28 attempting to access the device beyond 48 hours since the last time

1 the device was accessed. It is not known which finger(s) or thumb of  
2 which person(s) will unlock the device, but in any event all that  
3 would result from successive failed attempts is the requirement to  
4 use the authorized passcode or password.

5 **III. LEGAL DISCUSSION**

6 Compelling a person to provide a fingerprint or thumbprint as  
7 part of a search warrant violates neither the Fifth nor the Fourth  
8 Amendment.

9       **A. The Fifth Amendment Presents No Barrier to Obtaining a**  
10       **Person's Fingerprints**

11 Compelling a person to provide his or her fingerprint does not  
12 implicate, let alone violate, the Fifth Amendment. "[B]oth federal  
13 and state courts have usually held that [the Fifth Amendment] offers  
14 no protection against compulsion to submit to fingerprinting."  
15 Schmerber v. California, 384 U.S. 757, 764 (1966). That is so  
16 because the Fifth Amendment privilege against self-incrimination only  
17 prevents the use against an accused<sup>1</sup> of testimonial or communicative  
18 evidence obtained from him. Id. As the Supreme Court explained in  
19 Schmerber, that prohibition does not apply to the use of a person's  
20 "body as evidence when it may be material." Id. at 763 (quoting Holt  
21 v. United States, 218 U.S. 245, 252-53 (1910)); see United States v.  
22 Dionisio, 410 U.S. 1, 5-6 (1973) ("It has long been held that the  
23 compelled display of identifiable physical characteristics infringes  
24 no interest protected by the privilege against compulsory self-  
25 incrimination."). The Ninth Circuit has held the same: "requests by

---

27       <sup>1</sup> It is, moreover, worth noting that the Fifth Amendment  
28 protects the accused, and as of this point, no person is being  
accused.

1 the prosecution for . . . fingerprint evidence from a defendant or a  
2 suspect are not prohibited by the Fifth Amendment right against self-  
3 incrimination because such evidence is not testimonial in nature."  
4 Commonwealth of Northern Mariana Islands v. Bowie, 243 F.3d 1109,  
5 1120 n.5 (9th Cir. 2001); see also United States v. De Palma, 414  
6 F.2d 394, 397 (9th Cir. 1969) ("Identifying physical characteristics  
7 are not evidence of a testimonial nature."); United States v. Sanudo-  
8 Duarte, 2016 WL 126283 (D. Ariz. 2016) (holding that defendant could  
9 be compelled to provide exemplar of his palm prints); Virginia v.  
10 Baust, CR14-1439 (Va. Cir. Ct. Oct. 28, 2014) (holding that defendant  
11 could be compelled to provide his fingerprint in order to unlock  
12 phone)

13 While the government does not know ahead of time the identity of  
14 every digital device or fingerprint (or indeed, every other piece of  
15 evidence) that it will find in the search, it has demonstrated  
16 probable cause that evidence may exist at the search location, and  
17 needs the ability to gain access to those devices and maintain that  
18 access to search them. For that reason the warrant authorizes the  
19 seizure of "passwords, encryption keys, and other access devices that  
20 may be necessary to access the device." A password, "key," or use of  
21 a fingerprint are all means of gaining access to other spaces or  
22 devices, and are seizable both to gain and maintain access. See,  
23 e.g., United States v. Shi, 525 F.3d 709, 731 (9th Cir. 2008)  
24 (authorizing seizure of keys and identification cards to show indicia  
25 of ownership); United States v. Honore, 450 F.2d 31, 33 (9th Cir.  
26 1971). The fact that a successful unlocking of the device could also  
27 demonstrate a connection between the person and the device thus does  
28 not make the requested fingerprints testimonial, any more than does a

1 warrant's authorization to seize a person's keys. If anything, the  
2 connection raises a Fourth Amendment concern, which is discussed and  
3 dispatched below. Finally, as law enforcement will only be seeking  
4 to depress the fingerprints of those persons present at the search  
5 location for whom law enforcement has cause to believe may be a user  
6 of a device, neither the Fifth nor Fourth Amendment is violated.

7       **B. The Fourth Amendment Permits the Acquisition of the**  
8       **Fingerprints**

9       The requested warrant also does not violate anyone's Fourth  
10 Amendment rights. It is true that the Fourth Amendment is implicated  
11 when the government seeks fingerprints for investigatory purposes.  
12 See, e.g., United States v. Parga-Rosas, 238 F.3d 1209, 1215 (9th  
13 Cir. 2001); but see Dionisio, 410 U.S. at 4 ("The Fourth Amendment  
14 prohibition against unreasonable search and seizure applies only  
15 where identifying physical characteristics, such as fingerprints, are  
16 obtained as a result of unlawful detention of a suspect, or when an  
17 intrusion into the body, such as a blood test, is undertaken without  
18 a warrant, absent an emergency situation."). But the Fourth  
19 Amendment's requirements are satisfied when the taking of  
20 fingerprints is supported by reasonable suspicion. See Hayes v.  
21 Florida, 470 U.S. 811, 817 (1985) ("There is thus support in our  
22 cases for the view that the Fourth Amendment would permit seizures  
23 for the purpose of fingerprinting, if there is reasonable suspicion  
24 that the suspect has committed a criminal act, if there is a  
25 reasonable basis for believing that fingerprinting will establish or  
26 negate the suspect's connection with that crime, and if the procedure  
27 is carried out with dispatch."); United States v. Garcia-Beltran, 389  
28 F.3d 864, 868 (9th Cir. 2004) ("[T]he Court has reaffirmed the

1 principle that the Fourth Amendment does not permit admission of  
2 fingerprint evidence resulting from a seizure without reasonable  
3 suspicion"); but see *Davis v. Mississippi*, 394 U.S. 721, 728 (1969)  
4 (holding that warrantless "dragnet" investigatory "[d]etentions for  
5 the sole purpose of obtaining fingerprints are no less subject to the  
6 constraints of the Fourth Amendment. It is arguable, however, that,  
7 because of the unique nature of the fingerprinting process, such  
8 detentions might, under narrowly defined circumstances, be found to  
9 comply with the Fourth Amendment even though there is no probable  
10 cause in the traditional sense.").

11       A fortiori, a search warrant based on probable cause, such as  
12 that sought here, would satisfy the Fourth Amendment, especially  
13 since law enforcement will not obtain the fingerprints from any  
14 person for whom they do not have cause to believe may be a user of a  
15 device. Because there is probable cause sufficient to seize the  
16 digital device, there is probable cause sufficient to seize "the key"  
17 to that device in the form of a person's fingerprint - similar to the  
18 provisions in the warrant to seize other keys. Moreover, while  
19 executing this provision of the search warrant may result in a brief  
20 detention of persons found at the Subject Premises, this too is  
21 consistent with Hayes because it will be done "with dispatch" and  
22 because it is done pursuant to the judicial authorization sought  
23 here. 470 U.S. at 814; see also Michigan v. Summers, 452 U.S. 692,  
24 705 (1981) (a valid search warrant implicitly carries with it the  
25 limited authority to briefly detain the occupants on, or in the  
26 immediate vicinity of, the premises while the search is being  
27 conducted); United States v. Broussard, 80 F.3d 1025, 1033 (5th Cir.  
28 1996) (holding that 10-to 15-minute detention of occupant was

1 reasonable while agents searched occupant's residence pursuant to  
2 valid search warrant).

3 IV. CONCLUSION

4 The government respectfully requests that the search warrant be  
5 issued with the procedures permitting the law enforcement personnel  
6 to depress the fingers of every person who is located at the SUBJECT  
7 PREMISES during the execution of the search and who is reasonably  
8 believed by law enforcement to be a user of a fingerprint sensor-  
9 enabled device that is located at the SUBJECT PREMISES and falls  
10 within the scope of the warrant.

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28



# **ATTACHMENT-1**

Friday, May 6, 2016

## Thumbprints to unlock phones can be compelled, courts say

By L.J. Williamson

Though the legal wrangling between Apple and the FBI over access to a San Bernardino mass shooter's iPhone has ended, new questions about permissible ways for police to gain access to phone data are being answered in lesser-known cases.

A search warrant issued in February by Central District Magistrate Judge Alicia G. Rosenberg authorized law enforcement personnel to depress the thumbprint of a Glendale woman onto the touch ID sensor of her iPhone so they could examine its contents. A previous ruling in *Virginia v. Baust*, (No. CR14-1439 Va. Cir. Oct. 28, 2014), held that a suspect "cannot be compelled [by the police] to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same."

The Virginia case hinged on the controversial definition of what comprises "testimonial communication." The court concluded that a passcode was entitled to Fifth Amendment protection because it only existed in the defendant's mind, and forcing him or her to speak the passcode to authorities would be a form of self-incrimination. Yet a fingerprint, which case law has likened to a key □ a physical object that can be handed over □ was not entitled to that same protection.

To some, focusing on the distinction between two different methods of obtaining the same result may seem forced.

"Despite the fact that it seems artificial, it's consistent with the approach the Supreme Court has taken to the Fifth Amendment," said Stanford law professor David Sklansky, citing the court's reasoning in *Pennsylvania v. Muniz* 496 U.S. 582 (1990), in which the court drew a sharp distinction between invading information from a suspect's mind versus demanding access to physical characteristics of his body. "The artificiality is in Supreme Court doctrine □ not in what the lower court did."

If police have a warrant, they have a legal right to search a phone, but that doesn't answer the problem of getting access to it, Sklansky explained. If police compel a user to place their thumb on a phone, it is compelling a suspect to do something with their body, much like compelling a suspect to stand in a lineup, and it does not impinge on the privilege against self-incrimination. "It's only compulsory self-incrimination if they get you to divulge the contents of your mind," Sklansky said. "A lot of people think it's artificial to draw the line that way, but that's what the Supreme Court says."

Albert Gidari, director of privacy at Stanford Law School's Center for Internet and Society, said the court is following a line of argument that the government likes to put forward, "there is nothing testimonial about unlocking a device you locked, whether it be by password, fingerprint, or otherwise."

It is compelled speech, however, Gidari argued. "It is akin to saying, 'Open up, it's me,' which raises Fifth Amendment issues."

The notion that biometrics generally are not testimonial, and that a fingerprint is akin to a hair sample or blood, is an "imperfect at best" analogy, Gidari said.

A better biometric analogy would be a voice print lock or an iris scanner, he said. "Could the court compel the person to state their password? Could a court force a person to look at the

camera? These methods unlock a device, but only after the person presents themselves and 'testifies' that they are the person with the right to access it ... The trend is against privacy here, but we don't have the last word on it yet."

Though she can see why law enforcement might want to make the distinction □ because it is more difficult to force someone to speak a passcode, invoking compelled speech and thought □ professor Jill Bronfman, director of the Privacy and Technology Project at UC Hastings College of the Law, said, "As a matter of access to data, passcodes are passcodes, regardless of the methodology or technology."

Yet at a future time, if biometric passcodes include wearable, implantable, and digestible biometric identifiers, compelling a suspect to divulge a passcode may seem tame by comparison, Bronfman said.

[lj\\_williamson@dailyjournal.com](mailto:lj_williamson@dailyjournal.com)